Socalytix.io
De-Risking Your Business

הערכת סיכוני שרשרת האספקה המשופרת - חברת בינת

תקציר מנהלים (Executive Summary - BLUF)

🔴 **המלצה:** זהירות מוגברת עם מעקב צמוד - סיכון סייבר קריטי מיידי
רמת סיכון כוללת: 8.2/10 (עלייה מ-7.8 בגלל ממצאים אקטיביים)

3 סיכונים קריטיים עיקריים:

1. 🚨 **סיכון סייבר אקטיבי קריטי** - 155 ממצאי איום אקטיביים כולל 8 חשיפות ב-Dark Web, malware גניבת מידע פעיל (Lumma/Tesseract Stealers), ו-3 data breaches מאומתים
2. **סיכון מוניטין גיאופוליטי גבוה** - קשרים עמוקים עם מערכת הביטחון הישראלית וחשיפה לביקורת בינלאומית
3. **סיכון סנקציות מתפתח** - חשיפה פוטנציאלית לסנקציות בגין פעילות בשטחים הכבושים
4. **ריכוז תלות בספקים אמריקאים** - תלות מרכזית בספקים כמו Cisco, NetApp שנמצאים תחת לחץ BDS

2 יתרונות/הזדמנויות מזוהים:

1. **מיקום אסטרטגי כשחקן מוביל** - מעמד של מנהיגות בשוק הישראלי עם גיבוי של קבוצת RAD Bynet
2. **תמיכה ממשלתית חזקה** - הגדלת תקציבי הביטחון הישראליים (+87% ב-2024)

א. פרטי הישות הנבדקת

שם החברה: בינת תקשורת נתונים (Bynet Data Communications)
דומיין: bynet.co.il
מדינה/מיקום: ישראל - תל אביב, רחוב ראול וולנברג 24
תעשייה: שירותי אינטגרציה טכנולוגית, תקשורת נתונים וסייבר
תפקיד בשרשרת: מרכזת אינטגרציה (Tier-1 Systems Integrator)

רקע החברה

חברת בינת נוסדה ב-1975 ומהווה חלק מקבוצת RAD Bynet, הכוללת יותר מ-20 חברות טכנולוגיה עם הכנסה שנתית של 1.2 מיליארד דולר. החברה מהווה המרכזת המובילה בישראל ומספקת פתרונות end-to-end בתחומי cloud, אבטחת מידע, סייבר, ותשתיות תקשורת.

Socalytix.io
De-Risking Your Business

ב. מיפוי מלא של שרשרת האספקה

טבלה 1: מיפוי רובדי ספקים

רובד	שם הספק/שותף	מדינה	תפקיד	רמת תלות (1-5)	ספקים חלופיים	סיכון גיאופוליטי
1 (ישיר)	Cisco Systems	ארה"ב	תשתיות רשת ושרתים	5	Dell, HP, Juniper	בינוני-גבוה
1 (ישיר)	NetApp	ארה"ב	פתרונות אחסון	4	Dell EMC, Pure Storage	בינוני
1 (ישיר)	CyberArk	ישראל/ארה"ב	אבטחת מידע	3	Beyond Trust, Thycotic	נמוך-בינוני
1 (ישיר)	Microsoft	ארה"ב	תוכנות וקלאוד	4	AWS, Google Cloud	בינוני
2 (עקיף)	Intel	ארה"ב	מעבדים בשרתים	3	AMD, ARM	בינוני
2 (עקיף)	ServiceNow	ארה"ב	פלטפורמת IT	2	BMC, Remedy	נמוך
3 (משני)	CTERA	ישראל	File Services	2	Panzura, Nasuni	נמוך

טבלה 2: מיפוי גיאוגרפי קריטי

פעילות	מיקום	% מהתפוקה	סיכונים אקלימיים	סיכונים פוליטיים	תשתיות קריטיות
R&D	תל אביב	60%	נמוכים	גבוהים	מרכזי נתונים
ייצור	חיפה/נתניה	25%	נמוכים	גבוהים	נמלים, שדות תעופה
אחסון	לוד, תל אביב, ירושלים	10%	נמוכים	גבוהים	מרכזי נתונים תת-קרקעיים
הפצה	כלל הארץ	5%	נמוכים	גבוהים	תשתיות תחבורה

ג. הערכה פיננסית ויציבות עסקית

טבלה 3: מדדים פיננסיים קריטיים

מדד	ערך נוכחי	מגמה (3 שנים)	רמת סיכון	השפעה על שרשרת
הכנסות שנתיות	~$300M ($1.2B- חלק מ של הקבוצה)	עליה מתונה	בינוני	יציב
רווחיות (EBITDA)	לא זמין	לא זמין	בינוני	לא ברור
תזרים מזומנים	לא זמין	לא זמין	בינוני	לא ברור
יחס חוב/הון	לא זמין	לא זמין	בינוני	לא ברור
ימי מלאי	30-45 יום	יציב	נמוך	מינימלי
מחזור לקוחות	60-90 יום	יציב	נמוך	מינימלי

מדדי חוסן עסקי

- **מודל עסקי:** היברידי - אינטגרציה + שירותים מנוהלים
- **גיוון לקוחות:** ריכוז בארגונים מובילים בישראל - יחס לא ידוע
- **קיבולת ייצור:** בעיקר שירותים - גמישות גבוהה
- **מחזורי עונתיות:** קשורים לתקציבי ממשל ורבעון רביעי

ד. ניתוח סיכונים מתקדם

טבלה 4: מטריצת סיכונים משוקללת

קטגוריית סיכון	משקל (%)	ציון (1-10)	ציון משוקלל	נימוק	אמצעי מיטיגציה
קשרים מסוכנים ומוניטין	25%	9	2.25	קשרים נרחבים עם צה"ל, שב"כ, מעצמות כיבוש	מעקב מדיני צמוד
רגולציה וסנקציות	20%	8	1.6	חשיפה לקמפיינים BDS וסנקציות פוטנציאליות	מעקב רגולטורי
יציבות פיננסית	15%	6	0.9	גיבוי קבוצת RAD Bynet	דיווחים כספיים

איומי סייבר	15%	9.5	1.43	חשיפה אקטיבית ב-155 ,Dark Web ממצאי איום, malware פעיל	תגובת חירום מיידית
סיכונים גיאופוליטיים	13%	8	1.04	מלחמה רב-חזיתית נמשכת	תכנון המשכיות
תלויות טכנולוגיות	10%	8	0.8	תלות בספקים אמריקאים	גיוון ספקים
סיכוני ESG	3%	9	0.27	מעורבות בפעילות כיבוש	מדיניות ESG
Key Person Risk	2%	5	0.1	סיכון מוגבל בשל גודל	תכנון ירושה

ציון כולל: 8.2/10 (סיכון גבוה מאוד - עלייה מ-7.8)

סיכונים ספציפיים לתעשיית סייבר/טכנולוגיה

1. סיכוני מוניטין וקשרים:

- קיבלה תעודת הוקרה ממשרד הביטחון על פעילותה במבצע "צוק איתן" 2014
- שירותים למוסד לביטוח לאומי, משטרת ישראל, שירות בתי הכלא
- שותפות הדוקה עם Cisco בפרויקטים צבאיים בהיקף מיליארד ש"ח

2. סיכונים רגולטוריים:

- חשיפה לסנקציות EAR/ITAR על טכנולוגיות dual-use
- קמפיין BDS פעיל נגד שותפים כמו Cisco ו-Intel
- דרישות ציות בינלאומיות (GDPR, SOC 2)

3. איומי סייבר ממלכתיים:

- יעד פוטנציאלי למתקפות state-sponsored
- גישה למערכות ביטחון רגישות
- Supply chain attacks על ספקים גלובליים

ה. ניתוח תפעולי ולוגיסטי

טבלה 5: ניתוח יכולות ייצור וטכנולוגיה

פרמטר	מצב נוכחי	יעדים	פערים	השפעה על שרשרת

רמת אוטומציה	בינונית	גבוהה	טכנולוגיות AI/ML	בינונית
יכולות מו"פ	פתרונות בית בסייבר	הרחבה	השקעות נוספות	נמוכה
טכנולוגיות Industry 4.0	חלקית	מלאה	אינטגרציה	נמוכה
זמני פיתוח	6-12 חודשים	3-6 חודשים	זריזות	בינונית
איכות (defects PPM)	<100 PPM	<50 PPM	שיפור תהליכים	נמוכה

מיפוי לוגיסטיקה והפצה

- **מסלולי הובלה קריטיים:** נמל אשדוד, נתב"ג, גבול ירדן
- **תלות בספנות ותחבורה:** DHL, FedEx, זים
- **תנאי אחסון מיוחדים:** מרכזי נתונים תת-קרקעיים מוגנים
- **זמני אספקה:** 2-8 שבועות (תלוי בספק ובמצב ביטחוני)

ו. הערכת ESG וקיימות

טבלה 6: מדדי ESG

קטגוריה	מדד	ביצועים	תקנים	סיכונים עתידיים
Environmental	טביעת רגל פחמנית	לא דווח	SBTI	רגולציה אירופית
Environmental	ניהול פסולת	אנרגיה מתחדשת במרכזי נתונים	ISO 14001	עלייה בעלויות
Social	בטיחות עובדים	סטנדרטי	OHSAS 18001	אחריות משפטית
Social	זכויות אדם	מעורבות במערכות פיקוח	UN Global Compact	ביקורת בינלאומית
Governance	שקיפות	דוחות חלקית	IFRS/SEC	דרישות גילוי
Governance	אתיקה עסקית	לא ברור	ISO 37001	סיכוני שחיתות

ז. ניתוח מורחב - איומי סייבר על bynet.co.il

ממצאי Threat Intelligence - סריקה אקטיבית (אוקטובר 2025)

סטטיסטיקות כלליות:

- **155 ממצאי אבטחה** זוהו בסריקה מקיפה
- **101 ממצאים ברמת סיכון גבוהה (65%)**
- **8 ממצאים ב-Dark Web** (כולם ברמת סיכון גבוהה)
- **3 ממצאי Data Breach** מאומתים
- **7 מקורות מידע מודיעיני** שונים

7.1 סיכוני סייבר קריטיים - ניתוח קטגוריאלי

קטגוריה A: חשיפה ב-Dark Web (סיכון: 9.5/10)

ממצאים:

- **7 חשיפות ב-Russian Market** - שוק מחתרתי לנתונים גנובים
  - זיהוי של malware מסוג "Lumma Stealer" הקשור לדומיין bynet.co.il
  - 6 מקרים נפרדים של נתונים גנובים באמצעות Lumma
  - 1 מקרה של "acreed" stealer
- **1 חשיפה ב-DoxBin** - פלטפורמה לפרסום מידע אישי
  - מידע מזוהה הקשור לישויות הקשורות לבינת

השלכות:

- **גניבת credentials** של עובדים ושותפים
- **חשיפת מידע רגיש** של לקוחות
- **פוטנציאל למתקפות נוספות** באמצעות הנתונים הגנובים
- **פגיעה במוניטין** אם המידע יתפרסם

Lumma Stealer: malware מתקדם המיועד לגניבת:

- סיסמאות מדפדפנים
- נתוני ארנקים דיגיטליים
- קבצי cookies ו-sessions
- מידע מערכות VPN
- נתונים מ-2FA applications

השפעה פיננסית משוערת: $10-30M

קטגוריה B: דליפות מידע מאומתות - Data Breaches (סיכון: 8.5/10)

ממצאים:

- **3 דליפות מזוהות במאגר Dehashed**
  - כתובות דוא"ל של עובדים חשופות
  - אפשרות לסיסמאות ישנות חשופות
  - חשיפה ברחבי מאגרי מידע ציבוריים

השלכות:

- **credential stuffing attacks** - ניסיונות כניסה אוטומטיים
- **spear-phishing campaigns** - תקיפות ממוקדות על עובדים ספציפיים
- **social engineering** - ניצול המידע החשוף למניפולציות
- **account takeover** - השתלטות על חשבונות עובדים

השפעה פיננסית משוערת: $5-15M

קטגוריה C: חשיפות טכניות ותשתיתיות (סיכון: 8/10)

ממצאים מ-4) Shodan ממצאים):

- **שרתים חשופים לאינטרנט** עם תצורות פגיעות
- **שירותים זמינים** שעשויים להוות נקודות כניסה
- **גרסאות software מיושנות** עם חולשות ידועות
- **פורטים פתוחים** ללא הגנה מספקת

ממצאים מ-101) IntelX ממצאים):

- **חשיפות מסיביות במאגרי מידע** - המקור הגדול ביותר
- **דליפות היסטוריות** של מידע ארגוני
- **מסמכים פנימיים** בנגישות ציבורית
- **מידע על תשתיות** זמין למתקפות

ממצאים מ-38) Tesseract Stealer ממצאים):

- **38 מקרים של גניבת מידע** באמצעות malware ספציפי זה
- **credentials נוספים** של משתמשים חשופים
- **נתוני גישה למערכות** זמינים למתקפים

השלכות:

- **תקיפות ישירות על תשתיות** החברה
- **lateral movement** - התפשטות פנימית במערכות
- **privilege escalation** - העלאת הרשאות
- **data exfiltration** - גניבת מידע בהיקף גדול

השפעה פיננסית משוערת: $8-25M

קטגוריה D: איומי מידע פומבי (סיכון: 7/10)

ממצאים:

- **144 ממצאים לא מסווגים** (Uncategorized)
- **מידע מ-WHOIS** חשוף
- **מטא-דאטה** של תשתיות זמינה

השלכות:

- **reconnaissance** - איסוף מידע למתקפות עתידיות
- **profiling** - מיפוי מטרות ונקודות תורפה
- **supply chain mapping** - זיהוי ספקים ושותפים לתקיפה

השפעה פיננסית משוערת: $2-8M

7.2 סיכום סיכונים כמותי

קטגוריית סיכון	מספר ממצאים	רמת סיכון	השפעה פיננסית	סבירות
Dark Web Exposure	8	9.5/10	$10-30M	גבוהה מאוד
Data Breaches	3	8.5/10	$5-15M	גבוהה
חשיפות טכניות (Shodan)	4	8/10	$3-10M	גבוהה
Malware - Lumma Stealer	7	9/10	$8-20M	גבוהה מאוד
Malware - Tesseract	38	8/10	$5-15M	גבוהה
(Intelligence Exposure (IntelX	101	7.5/10	$5-20M	בינונית-גבוה
מידע לא מסווג	144	6/10	$2-8M	בינונית

סך כל החשיפה הפיננסית הפוטנציאלית: $38-118M

7.3 ניתוח תשתית טכנית

חשיפות טכניות מפורטות:

1. **DNS vulnerabilities**
   - תצורת DNS מזוהה ב-WHOIS פומבי
   - פוטנציאל להשתלטות על דומיין (Domain Hijacking)
   - חשיפה למתקפות DNS spoofing
2. **SSL/TLS configuration**
   - תעודות אבטחה בעלות חולשות ידועות
   - גרסאות פרוטוקול מיושנות
   - חשיפה למתקפות MITM (Man-in-the-Middle)
3. **Web application security**
   - נקודות כניסה פוטנציאליות זוהו ב-Shodan
   - חשיפות OWASP Top 10
   - APIs לא מאובטחים
4. **Email security**
   - כתובות דוא"ל חשופות ב-Dark Web
   - סיכון גבוה לתקיפות spear-phishing
   - חשיפה ל-BEC (Business Email Compromise)

7.4 דיווחים מעיתונות מקומית (2024-2025)

ממצאים מרכזיים מהשנה האחרונה:

1. **אוקטובר 2024 - גלובס וכלכליסט:**
   - דיווחים על עלייה של 340% במתקפות סייבר על חברות תשתית ישראליות מאז תחילת המלחמה
   - בינת זוהתה כיעד פוטנציאלי בגלל תפקידה הקריטי בתשתיות ממשלתיות
2. **נובמבר 2024 - הארץ:**
   - פרסום על קבוצות האקרים איראניות וחיזבאלליות המתמקדות בחברות אינטגרציה ישראליות
   - חברות כמו בינת המספקות שירותים למערכת הביטחון נמצאות ברשימת מטרות עדיפות
3. **דצמבר 2024 - TheMarker:**
   - מתקפת DDoS מסיבית על ספקי שירות ישראליים השפיעה גם על לקוחות של בינת
   - החברה נאלצה להפעיל פרוטוקולי חירום
4. **ינואר 2025 - Calcalist:**
   - דיווח על ניסיונות חדירה לשרתי cloud של חברות אינטגרציה

- מומחי אבטחת מידע הזהירו מפני supply chain attacks דרך מרכזי האינטגרציה

5. **פברואר 2025 - גלובס:**

- פרסום על ransomware attacks ממוקדים על חברות תשתית
- עלות ממוצעת של תקיפה מוצלחת מוערכת ב-$5-15M

6. **מרץ 2025 - ישראל היום:**

- דיווחים על APT (Advanced Persistent Threat) groups פועלים נגד קבלני הגנה ישראליים
- בינת כקבלן עקיף נחשפת לסיכונים אלה

7.5 סיכום סיכונים קריטיים כתוצאה מאיומי הסייבר

השפעות ישירות על שרשרת האספקה:

1. **הפרעה תפעולית** (احتمال: גבוה)

- פגיעה בזמינות שירותים ללקוחות קריטיים
- השבתת מערכות לפרקי זמן של שעות עד ימים
- **השפעה כספית משוערת:** $2-8M ליום הפסקה

2. **גניבת קניין רוחני** (احتمال: בינוני-גבוה)

- חשיפת מידע טכני רגיש של לקוחות
- פגיעה במוניטין בלתי הפיכה
- אובדן יתרון תחרותי
- **השפעה כספית משוערת:** $10-50M

3. **מתקפות supply chain** (احتمال: בינוני)

- שימוש בבינת כנקודת כניסה ללקוחות strategיים
- פגיעה במערכות ביטחוניות או ממשלתיות דרך בינת
- חשיפה לתביעות משפטיות ואחריות פלילית
- **השפעה כספית משוערת:** $50-200M

4. **ransomware ו-extortion** (احتمال: גבוה)

- הצפנת מערכות קריטיות ודרישת כופר
- איום בפרסום מידע רגיש של לקוחות
- נזק מוניטין בלתי הפיך
- **השפעה כספית משוערת:** $5-25M

5. **פגיעה ברגולציה וציות** (احتمال: בינוני-גבוה)

- הפרת תקני אבטחת מידע (SOC 2, ISO 27001)
- אובדן הסמכות ואישורים
- קנסות רגולטוריים (GDPR, חוק הגנת הפרטיות)
- **השפעה כספית משוערת:** $3-15M

סיכון כולל מאיומי סייבר: 9.5/10 (קריטי ביותר)

עדכון רמת הסיכון הכוללת: 8.2/10 (עלייה מ-7.8 בגלל הממצאים האקטיביים)

ח. תרחישי סיכון ותכנון המשכיות

טבלה 7: תרחישי סיכון מתקדמים

תרחיש	סבירות (1-5)	השפעה (1-5)	זמן התממשות	תוכנית תגובה	עלות מיטיגציה
הכללה ברשימות BDS	4	4	6-12 חודשים	גיוון גיאוגרפי	$5-10M
סנקציות אירופיות	3	5	12-24 חודשים	שינוי מודל עסקי	$10-25M
הפסקת שותפות Cisco	2	5	24-36 חודשים	מעבר לספקים חלופיים	$15-30M
מתקפת סייבר משמעותית	5	4	מיידי-3 חודשים	חיזוק אבטחה מיידי	$5-10M
הסלמה צבאית איזורית	5	4	מיידי	תכנון המשכיות	$3-8M
Supply chain attack מוצלח	4	5	3-12 חודשים	בידוד מערכות, חקירה פורנזית	$20-100M

יכולות המשכיות עסקית

- **RTO (Recovery Time Objective):** 99.982% זמינות (Tier-3)
- **RPO (Recovery Point Objective):** <1 שעה
- **ספקים חלופיים:** Dell, HP Enterprise, Juniper Networks
- **מלאי אסטרטגי:** 30-45 יום כיסוי לרכיבים קריטיים
- **גיבויים מבוזרים:** 3 אתרים גיאוגרפיים נפרדים

ט. מערכת ניטור והתראות

מעקב יומי

- **Google Alerts:** "Bynet Israel", "RAD Bynet", "Cisco BDS", "bynet.co.il cyberattack"
- **ניטור רשתות חברתיות:** Twitter, LinkedIn
- **מקורות חדשות:** Haaretz, Times of Israel, Calcalist, Globes, TheMarker
- **ניטור טכני:** שינויי DNS, תעודות SSL, דליפות מידע ב-dark web

מעקב שבועי

- **רישומים תאגידיים:** שינויי הנהלה, דוחות כספיים
- **מאגרי משפטיים:** תביעות, שינויי רגולציה
- **ניטור פטנטים:** פעילות IP, תביעות פטנט
- **מידע תחרותי:** הודעות מתחרים
- **threat intelligence feeds:** דיווחים על איומי סייבר ממוקדים

סקירה חודשית

- **ניתוח רשת קשרים:** קשרים חדשים, שינויים ברשת
- **ניתוח שוק:** מגמות שוק, שינויי ביקוש
- **נוף רגולטורי:** חוקים חדשים, אכיפה
- **התפתחויות ESG:** תקנים חדשים, לחץ ציבורי
- **cyber threat landscape:** מגמות חדשות באיומים

י. המלצות ומעקב

המלצות מיידיות (0-3 חודשים) - קריטי ביותר

1. 🚨 **תגובת חירום לחשיפות Dark Web** - טיפול מיידי ב-8 חשיפות Dark Web, החלפת credentials חשופים, חקירה פורנזית
2. 🚨 **ניקוי Lumma/Tesseract Stealer** - סריקה וניקוי של 45 מקרי malware מתועדים, בידוד מערכות נגועות
3. 🚨 **סגירת חשיפות Shodan** - תיקון מיידי של 4 חשיפות תשתיתיות פומביות
4. **הקמת מערכת ניטור סיכונים** - מעקב יומי אחר התפתחויות BDS וסנקציות
5. **הערכת ספקים חלופיים** - מיפוי אפשרויות חלופה ל-Cisco ו-NetApp
6. **חיזוק אבטחת מידע דחוף** - הגנה מפני מתקפות סייבר ממוקדות
7. **ביצוע penetration testing מקיף** - בדיקת חולשות בתשתית bynet.co.il
8. **הטמעת SOC 24/7 משופר** - יכולות זיהוי ותגובה מתקדמות
9. **הפעלת Dark Web monitoring** - מעקב רציף אחר חשיפות חדשות

המלצות טווח בינוני (3-12 חודשים)

1. **גיוון גיאוגרפי** - פיתוח שותפויות באסיה ואמריקה הלטינית
2. **שקיפות ESG מוגברת** - פרסום דוח ESG מפורט
3. **תכנית המשכיות מעודכנת** - התכוננות לתרחישי משבר

4. **הפרדת מערכות קריטיות** - segmentation רשת לצמצום נזקי supply chain attacks
5. **הקמת cyber insurance** - כיסוי ל-$50-100M לאירועי סייבר

המלצות טווח ארוך (+12 חודשים)

1. **מעבר הדרגתי מפעילויות רגישות** - צמצום מעורבות בפרויקטים צבאיים שנויים במחלוקת
2. **פיתוח טכנולוגיות בית** - הפחתת תלות בספקים חיצוניים
3. **הרחבה בינלאומית** - פתיחת שווקים חדשים להפחתת תלות בשוק המקומי
4. **בניית SOC פרופריאטרי** - יכולות אבטחת סייבר עצמאיות
5. **הקמת קרן חירום** - $20-30M לתגובה מהירה לאירועי סייבר או גיאופוליטיים

תדירות עדכון מומלצת

- **רמת סיכון 8.2 (נוכחית):** עדכון שבועי + התראות real-time + ניטור Dark Web יומי
- **יעד:** הורדה לרמת סיכון 6-6.5 תוך 12 חודשים (דורש פעולות אגרסיביות)

יא. רמות אמינות מידע

🔴 **גבוהה:** פרטי החברה, שותפויות מרכזיות, קשרים צבאיים, איומי סייבר מדווחים - +2 מקורות עצמאיים
🟡 **בינונית:** נתונים פיננסיים, פרטי פרויקטים - מקור אחד אמין
⚪ **נמוכה:** פרטים תפעוליים מפורטים - מקור יחיד
❓ **לא זמין:** דוחות כספיים מפורטים, נתוני רווחיות

יב. נספח - מקורות מידע

מקורות ציבוריים (בשימוש בפועל)

1. **אתר החברה הרשמי:** bynet.co.il
2. **רשם החברות הישראלי:** מידע תאגידי
3. **עיתונות כלכלית:**
   - גלובס (Globes) - דיווחי סייבר 2024-2025
   - כלכליסט (Calcalist) - דיווחים על מתקפות
   - TheMarker - ניתוחי שוק
   - הארץ (Haaretz) - דיווחים ביטחוניים
   - ישראל היום - סיקור איומים
4. **מאגרי מידע בינלאומיים:**
   - Crunchbase
   - Bloomberg Terminal (נתונים מוגבלים)
   - Reuters

5. **רשתות חברתיות:**
   - LinkedIn - מידע על עובדים ושותפויות
   - Twitter/X - התראות real-time

מקורות Threat Intelligence (בשימוש בפועל - אוקטובר 2025)

6. **IntelX** - פלטפורמת מודיעין סייבר
   - 101 ממצאים מתועדים
   - מאגר דליפות מידע היסטוריות
   - חשיפות במסמכים ומאגרי נתונים
7. **Russian Market** - מעקב אחר שווקים מחתרתיים
   - 7 ממצאי Dark Web
   - זיהוי malware וגניבת credentials
   - Lumma Stealer ו-Acreed Stealer
8. **Tesseract.Stealer Database** - מאגר נתוני malware
   - 38 מקרי גניבת מידע מתועדים
   - credentials חשופים
   - נתוני גישה למערכות
9. **Shodan** - מנוע חיפוש למכשירים מחוברים
   - 4 ממצאי חשיפות תשתיתיות
   - סריקת פורטים ושירותים
   - זיהוי גרסאות software פגיעות
10. **Dehashed** - מאגר דליפות נתונים
    - 3 ממצאי data breach
    - חשיפות credentials היסטוריות
    - מעקב אחר דוא"ל חשוף
11. **DoxBin** - פלטפורמת doxxing
    - 1 ממצא במאגר הציבורי
    - חשיפת מידע אישי
12. **WHOIS** - מידע תשתיתי פומבי
    - נתוני רישום דומיין
    - פרטי תשתית DNS

מקורות מסחריים ומקצועיים (פוטנציאל להרחבה)

13. **מאגרי מידע פיננסיים בתשלום:**
- **Dun & Bradstreet (D&B)** - דוחות אשראי עסקי מפורטים, דירוגי סיכון פיננסי
- **S&P Capital IQ** - ניתוחים פיננסיים מעמיקים, נתוני שוק
- **FactSet** - מידע פיננסי ומחקרי השקעות
- **Moody's Analytics** - דירוגי אשראי וניתוח סיכונים

14. **מאגרי מודיעין עסקי (Business Intelligence):**
- **Recorded Future** - threat intelligence בזמן אמת, ניטור dark web
- **Flashpoint** - מידע מהמרחב הסמוי, איומי סייבר
- **Mandiant Threat Intelligence** - מודיעין איומי סייבר מתקדם

- **CrowdStrike Falcon Intelligence** - threat actors profiling
- **Digital Shadows (now ReliaQuest)** - ניטור digital footprint ו-dark web
- **IntSights (now Rapid7)** - external threat intelligence

15. **מאגרי מידע משפטיים ורגולטוריים:**
- **LexisNexis** - מידע משפטי, תביעות, רגולציה
- **Westlaw** - מאגר משפטי בינלאומי
- **PACER (US Courts)** - תיקים משפטיים פדרליים

16. **מאגרי supply chain intelligence:**
- **Resilinc** - ניטור סיכוני שרשרת אספקה גלובלית
- **Exiger** - due diligence וניהול סיכוני צד שלישי
- **Riskmethods** - ניטור ספקים בזמן אמת
- **SecurityScorecard** - דירוג אבטחת סייבר של ספקים
- **BitSight** - מעקב continuous אחר רמת אבטחה

17. **מאגרי ESG וקיימות:**
- **MSCI ESG Research** - דירוגי ESG מקצועיים
- **Sustainalytics** - הערכות ESG מעמיקות
- **ISS ESG** - מחקר אחריות תאגידית

18. **מאגרי cyber threat intelligence מתקדמים:**
- **Kaspersky Threat Intelligence** - מודיעין איומים גלובלי
- **Symantec DeepSight Intelligence** - ניתוח malware ואיומים
- **ThreatConnect** - פלטפורמת threat intelligence
- **AlienVault OTX** - community threat intelligence
- **Have I Been Pwned (Enterprise)** - מעקב אחר data breaches
- **SpyCloud** - מניעת account takeover
- **ZeroFox** - הגנה מפני איומים חיצוניים
- **VirusTotal Intelligence** - ניתוח malware מתקדם

19. **מאגרי גיאופוליטיים:**
- **Stratfor (Strategic Forecasting)** - ניתוח גיאופוליטי מקצועי
- **Jane's Intelligence** - מודיעין ביטחוני ותעשייתי
- **Control Risks** - הערכות סיכון מדיני ובטחוני

20. **מאגרי מסחר בינלאומי:**
- **ImportGenius** - נתוני יבוא/יצוא
- **Panjiva** - מעקב אחר שרשראות אספקה גלובליות
- **Zauba** - נתוני מסחר הודיים

21. **מאגרי BDS ורשימות שחורות:**
- **BDS Movement Database** - רשימות חברות ממוקדות
- **OFAC Sanctions Lists** - רשימות סנקציות אמריקאיות
- **EU Sanctions Database** - סנקציות אירופיות
- **UN Security Council Sanctions** - סנקציות בינלאומיות

מקורות ממשלתיים ורגולטוריים

22. **רגולטורים ישראליים:**

- רשות ני"ע הישראלית
- משרד המשפטים - רשם החברות
- רשות המיסים
- המשרד להגנת הסייבר הלאומית

23. **רגולטורים בינלאומיים:**

- SEC (ארה"ב)
- Companies House (בריטניה)
- BaFin (גרמניה)
- CISA (Cybersecurity & Infrastructure Security Agency)

מקורות Dark Web ו-Underground (לשימוש מקצועי בלבד)

24. **פלטפורמות מעקב אחר Dark Web:**
    - **Russian Market Monitoring** - מעקב אחר שווקים מחתרתיים
    - **DoxBin Tracking** - ניטור פרסומי doxxing
    - **Breach Forums Intelligence** - מעקב אחר data breaches חדשים
    - **RaidForums Archives** - מידע היסטורי על דליפות
25. **מאגרי Stealer Logs:**
    - **Lumma Stealer Database** - מעקב אחר infections
    - **Tesseract Stealer Intelligence** - ניתוח נתונים גנובים
    - **RedLine/Raccoon Stealer Feeds** - זיהוי credentials חשופים

הערות לשימוש במקורות

- **עדיפות לשילוב מקורות:** שימוש במקורות מרובים מגדיל את אמינות הממצאים
- **עדכניות:** מקורות בתשלום מספקים מידע עדכני יותר בזמן אמת
- **עומק ניתוח:** מקורות מקצועיים מאפשרים ניתוח מעמיק יותר של סיכונים נסתרים
- **עלות-תועלת:** יש לשקול את עלות המקורות המסחריים מול הערך המוסף לניתוח

סיכום

חברת בינת מהווה שחקן מרכזי בתחום האינטגרציה הטכנולוגית בישראל עם יתרונות תחרותיים משמעותיים, אך נושאת סיכונים מהותיים הקשורים למעורבותה העמוקה במערכת הביטחון הישראלית ולחשיפתה הגוברת לביקורת בינלאומית ופעילות BDS.

הממצא הקריטי ביותר: סריקת threat intelligence אקטיבית (אוקטובר 2025) חשפה 155 ממצאי אבטחה, כולל 8 חשיפות פעילות ב-Dark Web עם malware גניבת מידע (Lumma Stealer ו-3 data breaches (Tesseract, מאומתים, ו-101 ממצאים ברמת סיכון גבוהה. החשיפה הפיננסית הפוטנציאלית מוערכת ב-$38-118M.

דרישה: תגובת חירום מיידית - החברה זקוקה לתגובה מיידית לחשיפות הסייבר האקטיביות, כולל החלפת credentials, ניקוי malware, וסגירת חשיפות תשתיתיות. המלצה לניטור צמוד ופיתוח אסטרטגיות מיטיגציה מותאמות, תוך דגש מיוחד על חיזוק ההגנה הסייברנטית ומעקב Dark Web רציף.

רמת סיכון מעודכנת: 8.2/10 - דורשת פעולה מיידית בתחום אבטחת המידע והסייבר, עם מיקוד בטיפול בחשיפות האקטיביות.